NORTH DAKOTA

HOMELAND SECURITY

ANTI-TERRORISM SUMMARY

North Dakota State and Local Intelligence Center

NDSLIC

1-866-885-8295

The North Dakota Open Source Anti-Terrorism Summary is a product of the North Dakota State and Local Intelligence Center (NDSLIC). It provides open source news articles and information on terrorism, crime, and potential destructive or damaging acts of nature or unintentional acts. Articles are placed in the Anti-Terrorism Summary to provide situational awareness for local law enforcement, first responders, government officials, and private/public infrastructure owners.

NDSLIC Disclaimer

The Anti-Terrorism Summary is a non-commercial publication intended to educate and inform. Further reproduction or redistribution is subject to original copyright restrictions. NDSLIC provides no warranty of ownership of the copyright, or accuracy with respect to the original source material.

QUICK LINKS

North Dakota

Error sounds emergency sirens in Casselton. Repair crews in the North Dakota town of Casselton are trying to figure out why emergency sirens inexplicably went off October 23. Residents heard the tone of emergency sirens ringing throughout Casselton with no explanation. Public works crews were able to silence the sirens by manually disabling the siren. The Casselton auditor said a repair crew was on its way to the city, and she expects work to be finished by October 25. Source: http://bismarcktribune.com/news/state-and-regional/error-sounds-emergency-sirens-in-casselton/article_00a0baca-1e5a-11e2-b0c9-001a4bcf887a.html

Arizona pair due in ND court on bank fraud charges. Two executives from a defunct Arizona mortgage lender were due in a North Dakota federal court October 19 to hear charges against them alleging that they swindled Bismarck, North Dakota-based BNC National Bank out of at least $26 million. The two men are charged with conspiracy to commit bank fraud and wire fraud, and court records indicated they might enter pleas during the hearing. One was the CEO of American Mortgage Specialists Inc. (AMS) and the other was the company's vice president in charge of lending operations. Authorities said AMS defrauded BNC by providing it with false financial statements and other information about the status of loans the bank had financed. A printout obtained by a BNC employee in April 2010 showed that few loans at AMS remained to be sold, according to court documents. "The printout revealed that approximately $565,000 of loans remained to be sold, rather than the approximately $27 million of loans which were shown in BNC records as being held for sale to investors," a federal affidavit reads. "BNC ceased funding the loans, and AMS closed its operations." Source: http://www.sfgate.com/news/article/Arizona-pair-due-in-ND-court-on-bank-fraud-charges-3963573.php

Regional

(Minnesota) **Four months after being devastated by floods, popular Northland State park to reopen Monday.** Jay Cooke State Park in Minnesota was set to reopen October 22, 4 months after flooding washed away roads, trails, and bridges, Duluth News Tribune reported October 19. Park visitors, however, were restricted to driving into the park from the west, and only as far as park headquarters and the campground. Minnesota Highway 210 was expected to be fully reopened to the public by 2013 or 2014. By October 22, the park would reopen its office, interpretive center, campground, and camper cabins to the public. The June flooding washed out a 9-foot-diameter overflow pipe near the Thomson Bridge, and caused washouts and landslides along Highway 210, which is built on hills of unstable clay and silt in the park. The biggest problem was between park headquarters and Oldenburg Point, where floodwaters tore a 50-foot-deep, 250-foot-wide gap through the highway after an earthen embankment on Forbay Lake, a part of Minnesota Power's reservoir/power generation system, gave way. Minnesota Department of Transportation engineers and consultants were working to develop a solution for reopening the road. Minnesota Power was working with the Federal Energy Regulatory Commission planning the restoration of Forbay Lake. Source: http://www.duluthnewstribune.com/event/article/id/247015/group/homepage/

(Minnesota) **Drought brings pleas to cut back water use.** With rivers and rainfall approaching record low levels, Minnesota State officials said October 18 they want homeowners to eliminate “nonessential” water use, such as lawn watering and car washing, and have told farmers to abide strictly by irrigation permits. In parts of the State, some residential wells have run dry or had flow reduced by commercial and residential neighbors, said the deputy director of Ecological and Water Resources at the Department of Natural Resources (DNR). Continued lack of rain could prompt the DNR, under terms of a drought action plan, to require specific water conservation targets for users, particularly cities. In recent weeks it suspended 50 permits for surface water use by businesses, golf courses, and parks departments across the State, though many have backup water sources. The weekly update of the U.S. Drought Monitor noted a gradual retreat of drought conditions nationally, but an area of extreme drought broadened across southwest Minnesota. Nearly half the State was classed as experiencing extreme or severe drought, with a wide patch of northwestern Minnesota remaining in the extreme category. Source: http://www.startribune.com/local/174786211.html?refer=y

(South Dakota) **Flood repair work continues on the Missouri River.** Even though drought dropped levels in Missouri River reservoirs drastically, 2011’s flood damage is still being repaired at key points along the waterway, WNAX 570 AM Yankton reported October 24. Upriver, restoration is underway at Gavins Point Dam near Yankton, South Dakota. The dam’s operations manager said bank restoration work was being done just downstream from the dam on the north shore. “We lost about 12 foot of river bed there so we lost the foundation for that riprap,” he said. “That riprap work is going on and that’ll probably be going on for three or four more months.” The water releases during the summer of 2011 topped 160,000 cubic feet per second and caused damage along and under the concrete slab just in front of the spillway gates. The operations manager said repairs are planned for that area, too. Contractors would drill through the massive slab, working to fill some voids that developed in the gravel bed under the concrete as the floodwaters churned. Source: http://www.radioiowa.com/2012/10/24/flood-repair-work-continues-on-the-missouri-river/

National

Corps: Absolute flood protection along Missouri River is impossible. A U.S. Army Corps of Engineers report said that absolute flood protection along the Missouri River is impossible, so the basin needs to prepare and plan for flooding in the future, Homeland Security News Wire reported October 19. “All of us bear a shared responsibility for reducing flood risk,” the report said. The Corps said it bears responsibility for the Missouri River flood in 2011, and acknowledged that it is now responsible for implementing lessons learned from the flood. Victims and political leaders declared that a disaster like that should never happen again. The Corps, however, said it cannot guarantee that floods of such magnitude can be prevented. The report said that the system of dams, reservoirs, and levees generally functioned as designed and their management prevented nearly $8.2 billion in damage. Still, a number of improvements must be made to reduce the likelihood and consequences of future floods. The

Corps said it was on track to make improvements to weather forecasting, communications, collaborations, and additional changes to make sure the system is maintained and operated. Source: http://www.homelandsecuritynewswire.com/dr20121019-corps-absolute-flood-protection-along-the-missouri-river-is-impossible

International

Moscow police arrest internet scam suspects. Russian authorities charged nine West African immigrants with allegedly stealing $28.8 million from hundreds of foreign companies through what police described as an elaborate scheme using bogus passports bearing names that appeared very similar to those of major Russian companies like Gazprom, Rosneft, and Murmansk Shipping Company, the Wall Street Journal reported October 25. The alleged scam targeted firms dealing in minerals, oil and gas, and other commodities operating in the United States, the European Union, China and South-East Asia and had been going on for many years, Russia's interior ministry said in a statement. The alleged fraudsters managed the ruse by using the companies' Russian names on the bogus IDs, which tricked the companies into thinking they were actually doing business with real firms. Raids on the homes of seven of the suspects uncovered counterfeit documents, bogus notary stamps, falsified company paperwork, and printing equipment capable of producing it all, the police said. Investigators said the proceeds of the scam appeared to have been sent to Africa. Source: http://blogs.wsj.com/emergingeurope/2012/10/25/moscow-police-arrest-internet-scam-suspects/

Japan nuke plant water worries rise. Japan's crippled Fukushima Daiichi nuclear power plant is struggling to find space to store tens of thousands of tons of highly contaminated water used to cool the broken reactors, the manager of the water treatment team told the Associated Press October 25. About 200,000 tons of radioactive water is being stored in hundreds of tanks built around the plant. Operator Tokyo Electric Power Co. (TEPCO) already chopped down trees to make room for more tanks and predicts the volume of water will more than triple within three years. TEPCO is close to running a new treatment system that could make the water safe enough to release into the ocean. But in the meantime its tanks are filling up — mostly because leaks in reactor facilities are allowing ground water to pour in. Outside experts worry if contaminated water is released, there will be lasting impact on the environment. They fear, because of the reactor leaks and water flowing from one part of the plant to another, which may already be happening. Source: http://www.businessweek.com/ap/2012-10-25/ap-interview-japan-nuke-plant-water-worries-rise

Jordan disrupts major al-Qaeda terrorist plot. Authorities in Jordan disrupted a major terrorist plot by al-Qa'ida-linked operatives to launch near-simultaneous attacks on multiple civilian and government targets, reportedly including the U.S. Embassy in the capital, Amman, Jordan, Western and Middle Eastern officials said October 21. The Jordanian government issued a statement describing the plot and saying that 11 people with connections to al-Qa'ida's affiliate in Iraq have been arrested. The foiled attack, described as the most serious plot uncovered in Jordan since at least 2005, was viewed with particular alarm by intelligence agencies because of its sophisticated design and the planned use of munitions intended for the Syrian conflict — a new sign that Syria's troubles could be spilling over into neighboring countries, the officials said. The alleged plotters are Jordanian nationals. The officials said the group had amassed a stockpile of explosives and weapons from Syrian battlefields and devised a plan to use military-style tactics in a wave of attacks across Amman. The scheme called for multiple strikes on shopping centers and cafes as a diversionary tactic to draw the attention of police and security officials, allowing other operatives to launch attacks against the main targets, which included government buildings and embassies. A Western official briefed on details of the plot confirmed that the heavily fortified U.S. Embassy in Amman was among the targets. The Jordanian government's statement said its intelligence service had broken up a cell that had been planning the attacks since June, arresting 11 people described as "supporters" of al-Qa'ida in Iraq. The State Department had no immediate comment on the plot and declined to confirm or deny that the U.S. Embassy in Amman had been on the target list. Source: http://www.washingtonpost.com/world/national-security/jordan-disrupts-major-al-qaeda-terrorist-plot/2012/10/21/e26354b4-1ba7-11e2-9cd5-b55c38388962_story.html?hpid=z3

Banking and Finance Industry

Advanced malware allows cybercriminals to empty a bank account in one go. Security firm AVG released its Community Powered Threat Report for the third quarter of 2012. The study focuses on the 2.0 version of the Blackhole exploit kit, the evolution of malware and other threats that marked the past quarter. According to AVG, the Blackhole exploit kit leads both the toolkit and the malware markets with a share of almost 76 percent, respectively 63 percent. Considering that the crimekit's authors launched the 2.0 version, experts say its market share will grow even further and the attacks it utilizes in will become even more "aggressive" because of the advanced evasion techniques recently integrated into it. "Blackhole is a sophisticated and powerful exploit kit, mainly because it is polymorphic and its code is heavily obfuscated to evade detection by anti-virus solutions. The rapid update capabilities of the kit have also made it challenging for traditional antivirus vendors to track, which are the main reasons it has a high success rate," said the CTO at AVG Technologies. "Through our multi-layered security approach with real-time analysis at the endpoint, AVG has been detecting a much higher rate of Blackhole Toolkit-based attacks than other toolkits, as Blackhole's creator seeks to stay ahead of their competition," he added. Source: http://news.softpedia.com/news/Advanced-Malware-Allows-Cybercriminals-to-Empty-a-Bank-Account-in-One-Go-302135.shtml

ATMs may be top targets for crime: Verizon report. More than half of intrusions in the financial industry in a recent study led by Verizon involved tampering with ATMs, the company said in a report published October 24. Overall, 61 percent of security threats involved physical tampering, including the installation of skimming and camera devices on ATMs. Roughly one in four threats involved malware that captures user names and passwords. Another 22 percent involved hacking. According to the study, 56 percent of data breaches compromised ATMs. Another 21 percent of attacks compromised database servers, while 13 percent involved Web servers. Overall, 96 percent of threats to banks originated externally and emanated mostly from professional criminal organizations in Eastern Europe and elsewhere, according to the study.

Still, 9 percent of breaches involved employees of the target company, one of the highest rates of internal breaches among industries the group examined. Insiders were people who typically handled financial transactions, such as bank tellers and loan officers, the study found. Source: http://www.americanbanker.com/issues/177_206/atm-may-be-top-targets-for-crime-1053833-1.html

The FBI warns of dating extortion scams and payday loan schemes. The FBI's Internet Crime Complaint Center (IC3) issued an alert to warn Internet users about the new twists added by scammers to previously existing scams. The advisory comes after the agency received a large number of complaints from victims. The first type of improved scam detailed in the advisory refers to "dating extortion." In these plots, the criminals select their victims on online dating Web sites. After gaining their trust, the fraudsters attempt to convince users to take part in sexual conversations. Soon afterwards, the victims receive a text message with a link to a Web site that contains their names, phone numbers, photographs, and the adult-themed conversations they had with the con artist. These "cheater" Web sites offer customers the chance to purchase the conversations for $9. The information can also be removed from the site for $99. However, according to the victims' reports, the information was not removed from the Web sites even after the money was paid. Payday loan schemes are also highly common, but the "improved" variants do not just involve harassing phone calls, but also home visits from the so-called debt collectors. In these scams, victims are harassed in myriad ways about an alleged loan which they must repay. Although many of the targets of these plots never applied for payday loans, the con artists keep threatening them until they submit. Source: http://news.softpedia.com/news/The-FBI-Warns-of-Dating-Extortion-Scams-and-Payday-Loan-Schemes-301859.shtml

U.S. exchange flags internal trading discrepancy. U.S. exchange operator Direct Edge said October 22 that it found a discrepancy between how a stock trades in certain circumstances compared with what its rules state, a contradiction at the center of a growing debate over market complexity and fairness. The discrepancy that Direct Edge found in its mid-point-match (MPM) order types has existed since trading platform EDGX officially launched as a national securities exchange in July 2010, the company said in a notice to traders. An order type is the set of instructions that govern the price and other variables in stock transactions. The discrepancy involves the exchange's Rule 11.8(a)(2), which is supposed to assign priority to MPM orders over, among others, non-displayed limit orders. Direct Edge said EDGX usually assigns priority for MPM orders but it identified a circumstance in which the trading platform did not. In addition, the likelihood that MPM orders are executed and result in price improvement is higher because they automatically interact with displayed order flow. How often the trading priority that MPM was supposed to deliver but did not was not indicated in the trading notice. Source: http://www.reuters.com/article/2012/10/22/us-exchanges-directedge-idUSBRE89L15X20121022

One in four customers are card fraud victims, study finds. A new study looking at the behavior and concerns of customers worldwide concerning card fraud was released October 17 by payments solutions provider ACI Worldwide and the Aite Group, a research firm. The 2012 fraud report, titled "Global Consumers React to Fraud: Beware Back of Wallet," found that 27 percent of global consumers had been hit by credit card fraud over the past 5 years. Many of those who experienced fraud turned to using cash, checks, or other cards more after receiving a replacement card. The study found that 46 percent of customers who received a replacement card because of a data breach or other fraud activity used the card less than before. The study asked more than 5,200 customers in more than 17 countries around the globe if they had experienced card fraud and how that had changed their consumer behavior. The percentage of respondents who had experienced fraud in the last 5 years stayed consistent with the 2011 report findings, but there was a sharp increase in the number of respondents who had experienced fraud more than once in the last 5 years. This year 14 percent of the respondents had been victimized by fraudsters multiple times, compared to only 6 percent last year. Source: http://www.banktech.com/one-in-four-customers-are-card-fraud-vic/240009173

Ally Financial latest US bank to face cyber attacks. October 18, Ally Financial became the latest U.S. financial institution to face a cyberattack. Bank of America, Wells Fargo, and other banks in recent weeks have suffered so-called distributed denial-of-service (DDoS) attacks in which hackers use a high volume of incoming traffic to delay or disrupt customer Web sites. Regional bank BB&T and credit card issuer Capital One confirmed disruptions earlier the week of October 15. A spokeswoman for Ally said the bank was investigating the "unusual traffic" on its Web site. Banks have stressed that customer accounts and information was not at risk, but the attacks have highlighted the growing threat from hackers against U.S. infrastructure. Source: http://www.nbcnews.com/technology/technolog/ally-financial-latest-us-bank-face-cyber-attacks-1C6557410

HSBC Web sites fell in DDoS attack last night, bank admits. HSBC blamed a distributed denial-of-service (DDoS) attack for the downtime of many of its Web sites worldwide October 18. Readers told The Register that they were unable to reach the HSBC UK and First Direct Web sites, leaving them unable to carry out Internet banking services. The problems lasted for around 7 hours. In a statement, HSBC said attacks affected customers worldwide, and reassured clients that sensitive account data was not exposed by the attack. Security researchers analyzing the earlier attacks quickly came to the conclusion that they were largely powered by botnet networks of malware-infected PCs. An EMEA Solutions architect team lead at Arbor Networks said: "Recent attacks have used what we call multi-vector attacks, attacks which utilize a combination of volumetric, and application layer attack vectors. What we are seeing here are TCP, UDP, and ICMP packet floods combined HTTP, HTTPS, and DNS application layer attacks." Source: http://www.theregister.co.uk/2012/10/19/hsbc_ddos/

Chemical and Hazardous Materials Sector

Top executives at Kolon Industries indicted for stealing DuPont's Kevlar trade secrets. Kolon Industries Inc. and several of its executives and employees were indicted for allegedly engaging in a multi-year campaign to steal trade secrets related to DuPont's Kevlar para-aramid fiber and Teijin Limited's Twaron para-aramid fiber, the U.S. Department of Justice announced October 18. The indictment seeks forfeiture of at least $225 million in proceeds from the alleged thefts. "Kolon is accused of engaging in a massive industrial espionage campaign that allowed it to bring Heracron quickly to the market and compete directly with Kevlar," said a U.S. attorney. Headquartered in Seoul, South Korea, Kolon was indicted by a grand jury in Richmond, Virginia. The indictment charges Kolon with one count of conspiring to convert trade secrets, four counts of theft of trade secrets, and one count of obstruction of justice. Kevlar is produced by E.I. du Pont de Nemours and Company (DuPont), one of the largest chemical companies in the United States. Source: http://www.fbi.gov/richmond/press-releases/2012/top-executives-at-kolon-industries-indicted-for-stealing-duponts-kevlar-trade-secrets

Commercial Facilities

Barnes & Noble reports breach of U.S. customer credit card data. Retailer Barnes & Noble said customers who shopped at 63 of its stores as recently as September may have had their credit card information stolen, and that federal law enforcement authorities have been informed of the breach, Reuters reported October 24. All PIN pads at its 700 stores were disconnected by the close of business September 14 due to signs of tampering on some of the units, the company said in a statement. Stores in California, Connecticut, Florida, Illinois, Massachusetts, New Jersey, New York, Pennsylvania, and Rhode Island were affected, Barnes & Noble said. The company advised those who have swiped their cards at stores in the affected states to change their debit-card PIN numbers as a precaution, and to review their statements for unauthorized transactions. Still, the company said its customer database was secure, and that purchases made on the Barnes & Noble Web site, Nook e-reader, and Nook mobile apps were not affected. Source: http://www.reuters.com/article/2012/10/24/us-barnesnoble-breach-idUSBRE89N05L20121024

Communications Sector

HackRF Jawbreaker could bring low-cost wireless hacking to the masses. A researcher created a new radio called HackRF that is a kind of all-in-one hacker's dream with functionality to intercept and reverse-engineer traffic from a wide range of frequencies and sources. HackRF is the work of a researcher from Great Scott Gadgets, and the idea behind the project was to build a multipurpose transceiver that a user could attach to his computer and use as a "software-defined radio." He released the hardware specifications and the software for the radio, called HackRF Jawbreaker, on Github. The device has the ability to transmit and receive over a wide range of frequencies, covering a huge number of commercial devices. Source: http://threatpost.com/en_us/blogs/hackrf-jawbreaker-could-bring-low-cost-wireless-hacking-masses-102212

Amazon AWS goes down again, takes Reddit with it. October 22, several Web sites that use Amazon's AWS cloud-computing service for hosting, including Reddit, Coursera, Flipboard, FastCompany, Foursquare, Netflix, Pinterest, Airbnb, and more, were down as it experienced "degraded performance for a small number of EBS volumes in a single Availability Zone" in the northern Virginia zone. When problems began Amazon reported, "we are currently investigating degraded performance for a small number of EBS volumes in a single Availability Zone in the US-EAST-1 Region." Then, about an hour later, the company updated its Service

Health Dashboard: “We can confirm degraded performance for a small number of EBS volumes in a single Availability Zone in the US-EAST-1 Region. Instances using affected EBS volumes will also experience degraded performance.” Amazon updated their customers throughout October 22, before finally stating “we are continuing to restore impaired volumes and their attached instances.” While some Web sites, such as Reddit, were back up October 22, others that rely on AWS were reportedly still experiencing problems. Source: http://www.forbes.com/sites/kellyclay/2012/10/22/amazon-aws-goes-down-again-takes-reddit-with-it/

Huawei gear is secure, say U.S. network service providers. Responding to a congressional report warning U.S. businesses not to buy equipment from Huawei Technologies or ZTE, three U.S.-based telecommunications companies that use Huawei products said they take strong precautions to safeguard their networks, Computerworld reported October 22. The report, by the House Permanent Select Committee on Intelligence, said the possibility that the two Chinese companies have ties to the Chinese government raises the prospect that China is using their gear to conduct electronic espionage. After the report was issued, three Huawei customers — Clearwire, Cricket Communications, and Level 3 Communications — defended their choices. The Chinese government slammed the congressional report. A Commerce Ministry spokesman said in a statement that the report “was based on subjective suspicions and inaccuracies” and made “groundless accusations against China.” Source: http://www.computerworld.com/s/article/9232579/Huawei_gear_is_secure_say_U.S._network_service_providers?

Critical Manufacturing

Nissan recalls new Altima in U.S. on loose steering bolts. October 22, Reuters reported that Nissan is recalling 13,919 of its top-selling Altima sedans in the United States because bolts that may not have been tightened properly during production could fall off, increasing the risk of a crash, according to U.S. safety regulators. The Altima sedans are from the from the 2012 and 2013 model years and were made at the Nissan plant in Canton, Mississippi, from May 10 to July 26, Nissan North America told the National Highway Traffic Safety Administration (NHTSA). “Some of the subject vehicles may have been manufactured with four transverse link bolts and two power steering rack bolts that were not torqued to the proper specification,” Nissan told regulators in a letter NHTSA showed on its Web site. As a result, the bolts may shake loose during driving, the letter states, and drivers may notice rattling noise. There was no mention of any injuries or crashes as a result of this issue on the NHTSA Web site. Altima owners will be asked to bring their cars into Nissan dealerships, where the bolts will be torqued to the proper specification, NHTSA said. The cars are under warranty protection. Source: http://www.reuters.com/article/2012/10/22/us-nissan-recall-altima-idUSBRE89L0LD20121022

Feds probe complaints that Jeep Patriots stall. U.S. government safety regulators are investigating complaints that engines on Jeep Patriot SUVs can stall without warning at highway speeds, the Associated Press reported October 19. The problem caused one crash in which two people were hurt, according to documents posted on the National Highway Traffic Safety

Administration (NHTSA) Web site. The investigation affects about 112,000 Patriots from the 2011 and 2012 model years that were sold in the United States by Chrysler Group LLC, the maker of Jeeps, as well as 18,000 that were sold in Canada. NHTSA said that it received a dozen complaints about stalling. Ten of the incidents occurred while the Jeeps were going 65 miles per hour or faster. In eight cases the Patriots could not be restarted and had to be towed. Source: http://www.wavy.com/dpp/news/us_news/Feds-investigate-Jeep-Patriot-stalling-problem_63475413

Defense/ Industry Base Sector

Pentagon cyber-threat sharing program lost participants. A Department of Defense (DOD) effort designed to share information on computer threats with defense contractors lost members, InsideDefense reported. Five of the initial 17 members pulled out of the Defense Industrial Base Enhanced Cybersecurity Services group, a component of the department's cybersecurity information assurance program, a DOD spokesman confirmed. Under the initiative, the government fed threat signatures to Internet service providers that participating defense companies paid to scan their traffic and identify malware, Foreign Policy reported. The program, aimed at offering participants additional security protection, ran in pilot mode for nearly 2 years. "At the end of the operational pilot, one of the commercial service providers withdrew. During the operational testing of the pilot, five of the 17 DIB companies chose to withdraw and reallocate their resources to other corporate priorities," the DOD spokesman told InsideDefense. Four of the five companies that quit during the pilot are considering to rejoin a modified version of the program, Foreign Policy reported. In another arrangement, the companies would cut the ISPs as middlemen, receiving threat signatures straight from the government. DOD apparently is hosting a briefing in coming weeks to inform companies of the initiative, according to InsideDefense. Source: http://www.nextgov.com/cybersecurity/2012/10/pentagon-cyber-threat-sharing-program-lost-participants/59028/

Nuclear arms oversight difficulties persist, DOE auditors say. A need to mitigate the expense of efforts to update the U.S. nuclear weapons complex has posed a continuing challenge to the Department of Energy (DOE), its inspector general said in a report issued the week of October 15. Auditors said the department still faces the same difficulties they described in a separate assessment issued November 2011, the Albuquerque Journal reported October 25. Shortcomings in the department's oversight of hired firms continue to raise significant concern, the inspector general stated, noting that related problems extend to protection of DOE assets as well as projects aimed at ensuring the dependability of the country's atomic arsenal. The report reaffirmed a prior call for the department to eliminate redundant activities within the National Nuclear Security Administration, the semiautonomous DOE branch responsible for overseeing the country's nuclear weapons and related operations. Separately, DOE investigators described security matters as posing "a key management challenge," a move they attributed largely to a high-profile July break-in at the Y-12 National Security Complex in Tennessee. "Given the policy issues that have arisen as a result of this intrusion and the importance of ensuring the safe and secure storage of nuclear materials at department sites, we have elevated safeguards and security to the management challenges list," their report stated. Source: http://www.nti.org/gsn/article/nuclear-arms-oversight-difficulties-persist-doe-auditors/

Woman gets two years for exporting sensitive parts to Iran. A Taiwanese woman was sentenced October 24 in San Antonio to 2 years in federal prison for providing sensitive military parts to Iran that authorities claim might be used against the United States. She pleaded guilty in July to a conspiracy charge for circumventing regulations barring the export of certain materials to Iran, which is on a list of countries that the U.S. designates as state sponsors of terrorism. From October 2007 to June 2011, the woman worked with an accomplice from Iran and an accomplice from the United Arab Emirates. They reportedly bought or attempted to buy from companies around the world more than 105,000 parts, valued at about $2.6 million. The woman and her partners conducted 599 transactions with 63 different U.S. companies for parts without notifying them the items were being shipped to Iran. The parts included underwater locator beacons, crystal oscillators used in military and aerospace applications, test cells for measuring electromagnetic radiation, broadband high-range signal amplifiers, RF network design and spectrum management software, and other equipment for military applications made to withstand rugged conditions. Source: http://www.mysanantonio.com/news/local_news/article/Woman-gets-two-years-for-exporting-sensitive-3978433.php

Confused by Defense cyber threat alerts? A translation is on the way. October 19, Nextgov reported that an expanded information-sharing program will potentially allow more than 2,600 defense suppliers access to classified Defense Department communications with select companies about indications of cyber threats, partly by adding context understandable to a wider audience, officials with the contractor responsible for the ramp-up said. The defense industrial base collaboration initiative started as a pilot program during summer 2011. In May, the Pentagon allowed the whole industry to join. Participants receive disclosures when the military detects signs of unfolding malicious campaigns so that their in-house technical teams can take protective measures. The Defense Department also distributes reports about breaches participating companies have suffered, after deleting identifying information to avoid exposing the weaknesses of competitors. Source: http://www.nextgov.com/cybersecurity/2012/10/confused-defense-cyber-threat-alerts-translation-way/58906/

Emergency Services

Nothing Significant to Report

Energy

Midwest drought idles Georgia ethanol plant. Georgia's only major producer of corn ethanol is temporarily shutting down its plant near Camilla, Georgia, citing the impact the drought in the Midwest is having on corn prices. Southwest Georgia Ethanol LLC (SWGE) announced October

24, that 2012's poor harvest not only is resulting in negative "crush margins" — a term for profitability in the ethanol business — but also is producing lower quality corn. "SWGE modeled all possible scenarios of slowing production and deemed it in SWGE's best financial interest to idle production until the markets return to levels conducive to profits," the company wrote in a news release. Source: http://www.bizjournals.com/atlanta/news/2012/10/24/midwest-drought-idles-georgia-ethanol.html

Food and Agriculture

Smucker's Uncrustables sold to schools recalled. J.M. Smucker Co. of Orrville, Ohio, used peanut butter that was produced by Sunland Inc. in "limited production runs" of 72-count bulk packs of the sandwiches that went to schools under the National School Lunch Program, a Smucker's spokeswoman said in an email October 18. The company found no problems with the peanut butter, which was supplied by the U.S. Department of Agriculture, or the finished products after routine tests. However, the spokeswoman said Smucker's recently notified school customers that they should check if they have any sandwiches from the recalled lots; the recalled sandwiches have either expired or will expire soon. She said she did not immediately know how many sandwiches were involved. Source: http://vitals.nbcnews.com/_news/2012/10/18/14542685-smuckers-uncrustables-sold-to-schools-recalled?lite#__utma=238145375.289694522.1348658399.1350558446.1350644341.19&__utmb=238145375.1.10.1350644341&__utmc=238145375&__utmx=-&__utmz=238145375.1350644341.1

Government Sector (including Schools and Universities)

Vermont .gov Website blamed for spam. The head of Vermont's Department of Labor said the State is not taking any immediate action to disable code in its computers that allowed spammers the week of October 15 to send unwanted emails that appeared to come from the U.S. federal government and were sent to tens of thousands of consumers. The federal government uses the URL shortening service bit.ly to create short URLs for .gov and .mil Web addresses. The shortened URLs use the 1.USA.gov domain extension, which appeared in the spam message. The 1.USA.gov URL is designed only to redirect users to .gov and .mil Web sites. In most instances, governments disable open redirect to prevent redirected messages from being sent to non-.gov or non-.mil addresses. However, Vermont did not disable open redirect for its labor.vermont.gov site, and that allowed spammers to exploit it, resulting in unsolicited emails being sent to unsuspecting consumers, an analyst with an IT security provider said in a blog posting. The Vermont Labor commissioner said the State is in the processes of replacing the Labor Department's Web site, which could occur within weeks, and suggested the problem will vanish when the new Web site becomes active. The commissioner said the State did not take immediate action to disable open redirect because no real damage — which she defines as the unauthorized release of confidential and/or personally identifiable information — occurred.

"If there's a reason we need to pull it quicker, we can, but no one is advising that we have to do that," she said. Source: http://www.govinfosecurity.com/vermont-gov-website-blamed-for-spam-a-5222?rf=2012-10-24-eg

(New Mexico) **Suspects at large after shooting at Air Force baseannex.** A group of people got into a fight with a U.S. airman October 25 inside a gated housing area of an Air Force base in New Mexico. One of them grabbed his gun and shot him, police said. Authorities in Albuquerque were searching for the suspects. The airman was in stable and satisfactory condition, according to a spokesman for Albuquerque police. SWAT and K-9 units were helping in the search. The airman was on patrol in the Maxwell housing area of Kirtland Air Force Base, which is separate from the base itself, when he noticed the suspicious group and approached them, according to a base spokesman. Source: http://news.blogs.cnn.com/2012/10/25/suspects-at-large-after-shooting-at-air-force-base-annex/?hpt=hp_t3

(Ohio) **Elyria school safety system shuts down phone, Internet.** Schools in Elyria, Ohio, lost phone lines and Internet access October 18. Dust on a sensor set off a chain reaction that disabled computerized systems for the majority of the school day. While the district could still dial 9-1-1 in the event of an emergency, a non-existing emergency perceived by a state-of-the-art safety system crippled most land line communications in the district. The outage affected all of the district's buildings, except for the middle school, which had yet to be updated to a new phone system. Problems started when dust set off an advanced smoke alarm system's sensor tucked into the peak of the bell tower at the old Washington building at the new high school. The system, seeing the speck, believed it was detecting smoke and reacted as programmed, the superintendent said. It set off a series of silent alarms and shut down systems in the building to protect them from possible smoke or heat damage. It took the school's air conditioning and heating offline to avoid spreading "smoke" throughout the building. With the air conditioning off, the school's server room — responsible for keeping the district's network and voice over Internet protocol phone lines operating — heated up quickly, reaching as high as 140 degrees, the superintendent said. The outage lasted for nearly 8 hours. No damage was done to any of the school's systems, he said. Source: http://morningjournal.com/articles/2012/10/19/news/doc5080c79c57b68919820920.txt?viewmode=fullstory

Information Technology and Telecommunications

DoS vulnerability found in wireless chips used by Apple, HTC, Samsung, Ford, others. Researchers from Core Security's Core Impact team uncovered a remotely exploitable vulnerability in Broadcom BCM4325 and BCM4329 wireless chipsets that could be leveraged by cybercriminals to launch a denial-of-service (DoS) attack. According to advisories published by the U.S. Computer Emergency Readiness Team (US-CERT) and Core Security, the vulnerability is caused by an out-of-bounds read error condition that exists in the chips' firmware. Apparently, an attacker sending an RSN (802.11i) information element can cause the WiFi NIC to stop responding. The flaw affects Apple, HTC, Samsung, Acer, Motorola, LG, Sony Ericson, and Asus products, including iPhone 4, iPod 3G, Xoom, Galaxy Tab, Nexus S, and Evo 4G. The Ford Edge car is also affected. The experts notified Broadcom and although there were some communication problems, the company released an official statement to say a patch was developed. Since many of the affected products are out of service, the patch will be provided to customers on a case-by-case basis. Source: http://news.softpedia.com/news/DOS-Vulnerability-Found-in-Wireless-Chips-Used-by-Apple-HTC-Samsung-Ford-Others-302384.shtml

XSS attacks remain top threat to Web applications. Cross-site scripting (XSS) attacks remain the top threat to Web applications, databases, and Web sites, an analysis of 15 million cyberattacks in the third quarter of 2012 revealed. Other top attack techniques are directory traversals, SQL injections (SQLi), and cross-site request forgery (CSRF), according to the latest Web application attack report by cloud hosting firm FireHost. The increase in the number of cross-site attacks is one of the most significant changes in attack traffic between Q2 and Q3 2012, the report said. XSS and CSRF attacks rose to represent 64 percent of the group. XSS is now the most common attack type, with CSRF now in second. Source: http://www.computerweekly.com/news/2240168930/XSS-attacks-remain-top-threat-to-web-applications

Google Drive opens backdoor to Google accounts. The Windows and Mac OS X desktop clients for Google's Drive file storage and synchronization service open a backdoor to users' Google accounts which could allow the curious to access a Drive user's email, contacts, and calendar entries. The sync tool includes a "Visit Google Drive on the web" link which opens Drive's Web interface in the default browser and automatically logs the user in. Somewhat problematic is the fact that this session can then be used to switch to other Google services such as Gmail and Google Calendar. Even if the user explicitly logs out of the Google sites by clicking the "Sign out" link, the Drive client will open a new session without requiring a password. The desktop clients request login credentials only once, when they are first installed and launched. The backdoor is particularly problematic where a user shares their account with others or where a computer is not password protected. The link also makes accessing a user's Google account unnecessarily simple for trojans. Source: http://www.h-online.com/security/news/item/Google-Drive-opens-backdoor-to-Google-accounts-1735069.html

Experts locate dropper of Japanese malware responsible for making death threats. Approximately 10 days ago, a piece of malware making death and bomb threats online on behalf of its victims was discovered. Now, researchers from Symantec discovered the malicious element's dropper. The dropper of Backdoor.Rabasheeta — the component responsible for installing the payload onto the victim's computer — creates a registry to ensure that the main module is executed each time the device is activated. After it drops the main module and the configurations files that enable the threat to communicate with its command and control server, it removes itself from the infected computer. Backdoor.Rabasheeta has the capability to open a backdoor on the compromised device and allow its controller to take command of it. Source: http://news.softpedia.com/news/Experts-Locate-Dropper-of-Japanese-Malware-Responsible-for-Making-Death-Threats-301400.shtml

Experts develop malware that's capable of bypassing antivirus solutions. Security researchers developed a USB dropper/spreadecapable of bypassing all of the popular commercial antivirus products utilized by Internet users worldwide. The antivirus programs that currently exist are designed to identify threats based on their signatures or on their behavior. Normally, if the malwargets by one system, the other one should detect it. However, researchers demonstrated there is a way to create malicious elements that can spread from one computer to the other without being detected. A security researcher specialized in reverse engineering and software security created a virus whose behavior is not cataloged by any antivirus solution as being malicious. The purpose of this test malware was to copy a presumablmalicious file to a USB drive and create an autorun.inf file on the targeted device without being detected. The "malicious element" would constantly search for the presence of removable disks. If one is found, it would be scanned to determine if it is already infected. If it is not, the autorun.inf file and a malicious executable would be copied onto it. Source: http://news.softpedia.com/news/Experts-Develop-Malware-That-s-Capable-of-Bypassing-Antivirus-Solutions-300747.shtml

Cybercriminals found to sell access to servers housed by Fortune 500 companies. Security professionals often warn about the risks posed by using the Remote Desktop Protocol (RDP) service without making sure that it is properly secured. As it turns out, cybercriminals are relying on the servicto compromise machines and sell access to them via underground markets. A security journalist discovered a Russian Web site called dedicatexpress(dot)com, which claims to sell access to around 17,000 computers from all around the world. It appears these machines were compromised because their owners failed to set strong RDP passwords,allowing the attackers to easily take them over. Dedicatexpress(dot)com offers its services to anyone who is willing to contact the owner via instant messaging and pay aregistration fee of $20. Source: http://news.softpedia.com/news/Cybercriminals-Found-to-Sell-Access-to-Servers-Housed-by-Fortune-500-Companies-301104.shtml

Increase in drive-by attacks and infected emails. In August and September, the research team from Eleven, a German email security provider, recorded a significant increase in malware sent via email. The most significant growth was reported for drive-by attacks in which emails link to manipulated Web sites that infect the users' computers when opened in a browser. Between August and September, the number of such attacks increased more than 80-fold and their share of overall spam levels increased from 0.1 percent to 9.5 percent. However, that growth was not at the expense of "classic" malware email, which contains malware as an attachment: the number of malware emails increased by 119 percent in September and by 252.8 percent as compared to the same month in 2011. Virus outbreaks remained roughly at the previous month's level (–5.7 percent), but increased by 50.5 percent in August. The plus was 186.4 percent as compared to September 2011. Source: http://www.net-security.org/malware_news.php?id=2299

Fake Lookout Mobile Security update steals files from Android users. Lookout recently warned customers about an application on Google Play that mimicked an update for their Android application. Experts from TrustGo analyzed the threat after the malicious element was removed from the online store. According to researchers, once installed on an Android smartphone, the malware — Trojan!FakeLookout.A — was capable of stealing SMS and MMS messages and uploading them to a remote server via FTP. The trojan also sent its controllers a list of the files present on the device's SD card. Based on this list, cyber criminals could upload specific files. TrustGo experts accessed the FTP server on which the stolen files were stored and they found not only SMS messages but also some video files. The server, apparently located somewhere in Colorado, also hosts a malicious Web Site designed to drop a backdoor trojan. This Web Site serves the malware to Windows users and also to ones running Mac OS and Linux operating systems. Depending on the OS, the site drops a different trojan. The malware found on Google Play is just a part of a larger attack. Judging by the complexity of the campaign, it is likely the cybercriminals who orchestrate it will somehow resurrect the Android trojan and disguise it as another legitimate-looking app. Source: http://news.softpedia.com/news/Fake-Lookout-Mobile-Security-Update-Steals-Files-from-Android-Users-300603.shtml

'Major interruption' at GitHub as attackers launch DDoS. Code sharing repository GitHub was hit by a distributed denial-of-service (DDoS) attack, causing major disruptions to its services. GitHub began investigating the issue at 1:05 p.m. PST, and by 1:33 p.m. PST, alerted its community to the attack. By 3:52 p.m. PST, it rectified the issue and reported everything was operating normally. GitHub wrote on its status page that it was looking into implementing "additional mitigation strategies to harden ourselves against future attacks." GitHub also experienced a series of DDoS attacks in February, and like those previous attacks, no one is claiming responsibility for this latest disruption. Source: http://www.zdnet.com/major-interruption-at-github-as-attackers-launch-ddos-7000006030/

National Monuments and Icons

Nothing Significant to Report

Postal and Shipping

Nothing Significant to Report

Public Health

(Pennsylvania) **After HIPAA complaint, officials review emergency-alert system.** In the wake of an allegation that personal medical information was disclosed by the former police chief, Monroeville, Pennsylvania officials took a closer look at who receives emergency-alert information from the dispatch center via texts and emails, the Pittsburgh Tribune-Review reported October 25. The assistant police chief filed a written complaint that accused the former chief of passing along details about an emergency medical call to someone who was not involved in the emergency. The U.S. Department of Health and Human Services was asked in August to investigate the situation. The former chief retired in 2010 but remained on a list of first responders who receive direct alerts of fire and medical emergencies. When officials realized the first-responders list was outdated, the former chief and at least 10 other names were purged from the list, and direct texts and emails were put on hold for about a week as fire departments submitted new contact lists, said the current police chief. Though officials agree that the list should be updated from time to time, they maintained that the situation did not violate the Health Insurance Portability and Accountability Act (HIPAA), as is alleged in the complaint. Source: http://triblive.com/neighborhoods/2805293-74/list-chief-responders-emergency-fire-harvey-polnar-department-information-medical#axzz2AJjnhHtI

Providers angry, patients worried as FDA yanks 'incorrect' list of facilities receiving recalled meds. October 23, the U.S. Food and Drug Administration (FDA) removed a 28-page list of more than 1,200 facilities nationwide that it said received potentially dangerous injectable steroid from New England Compounding Center (NECC) from its Web site after it had "found some technical problems with the list and the data are incorrect." Tennessee Department of Health sent out a list of 74 facilities that the FDA said had received products from the company. A Tennessee Department of Health spokesman issued a follow-up release saying it now appears the information the State got from the FDA was incorrect. He called the mistake, which resulted in worried patients bombarding providers, "very frustrating." He believed NECC supplied the list the FDA released. A business manager for Dermatology Associates in Oak Ridge, Tennessee, which was on the list, said her office was swamped by patients calling and, if they could not get through on the phone, walking in, worried they were at risk. The "false information" the FDA provided "has really messed up our work," she said. The NECC recalled all its products after an outbreak of fungal meningitis was traced to a contaminated injectable steroid. Source: http://www.knoxnews.com/news/2012/oct/23/providers-angry-patients-worried-as-fda-yanks-of/

Meningitis probe could hit hospital drug supplies. The extended shutdown of a sister company of the pharmacy at the center of the deadly U.S. meningitis outbreak may exacerbate drug shortages for some hospitals and healthcare providers as the number of infection cases neared 300, U.S. health regulators said October 22. Ameridose, a drug manufacturer owned by the same people who own New England Compounding Center, or NECC, has been closed since October 10. It will remain shuttered until November 5, while authorities inspect the plant, at least temporarily cutting off supplies to its customers. NECC shipped thousands of potentially contaminated vials of a steroid used for injections to treat severe back pain. Some 14,000 patients may have been exposed to the medicine that has so far led to 23 deaths. Twelve additional fungal meningitis cases were reported October 22, bringing the total to 294 in 16 States, plus 3 cases of peripheral joint infection likely linked to the tainted steroid, according to the U.S. Centers for Disease Control and Prevention. Nine of the new cases were reported in Michigan, which has reported 63 infections and 5 deaths. Source: http://www.reuters.com/article/2012/10/22/us-usa-health-meningitis-shortages-idUSBRE89L18320121022

Transportation

TSA replaces backscatter scanners with millimeter wave scanners at some airports. The Transportation Security Administration (TSA) is replacing some backscatter scanners at large

U.S. airports with millimeter wave scanners, Homeland Security News Wire reported October 23. Backscatter scanners have drawn the criticism of travelers since they debuted a several years ago. Many travelers felt the scanners invaded their privacy and others were concerned about the radiation levels the scanners emit. KNSD 7 San Diego reported that TSA said the scanners were being replaced to make way for more efficient machines in an effort to make security checks faster at some of the larger airports around the country. Backscatter scanners were removed from major airports including Los Angeles International Airport, Chicago's O'Hare International Airport, and New York's John F. Kennedy International Airport. The backscatter scanners were still being used at some larger airports, but would mainly be relocated to smaller airports with less foot traffic. According to TSA, the new scanners — known as millimeter wave scanners — use a computer program to detect potential threats, while displaying an image of a traveler similar to a cartoon. TSA has insisted that the radiation the backscatter scanners emit have nothing to do with them being replaced; radiation experts believe the millimeter wave scanners are safer. Source: http://www.homelandsecuritynewswire.com/dr20121022-tsa-replaces-backscatter-scanners-with-millimeter-wave-scanners-at-some-airports

FAA needs data policy changes to better address accidents, finds GAO. The Federal Aviation Administration (FAA) needs to undertake steps to reduce accident rates and improve related data collection, says a report from the Government Accountability Office (GAO). In the report dated October 4, auditors note that most general aviation accidents are a result of pilot error. The FAA bases some its accident-reduction goals and efforts on defined accident rates and annual flight hours, but the GAO warns that "shortcomings in flight activity data" will make it difficult to achieve reductions in fatality rates among the riskier segments. The GAO report says the FAA needs more specific performance measurements for each program in its accident reduction strategy to better determine if goals are being met or if more actions are needed, which is important because current operations "may not meet the overall goal by 2018." This goal and others fall under several FAA initiatives including the renewal of the General Aviation Joint Steering Committee and the implementation of the Flight Standards Service's 5-year strategy, which involves a series of efforts around risk management, outreach, training, and safety promotion. To strengthen measurements and better evaluate program goals, the GAO suggests the FAA explore new ways to collect flight hours more often with methods that "minimize the impact on the general aviation community." This would allow the FAA to establish accident-reduction goals for each individual industry segment, making better use of its existing data and making the goals easier to manage and achieve. Source: http://www.fiercegovernment.com/story/faa-needs-data-policy-changes-better-address-accidents-finds-gao/2012-10-17

Water and Dams

Corps progressing on Missouri River repairs. In 2011, sections of Missouri River levees in southwest Iowa and northwest Missouri were in ruins. As soon as flood waters receded, the U.S. Army Corps of Engineers began planning construction projects, and mild fall and winter weather allowed contractors to make critical repairs before the spring snow melt and runoff season, the Sioux City Journal reported October 22. Levee breaches near Percival, Hamburg, and Rockport, Missouri, were all fixed by March, said the chief of the Corps of Engineers' Omaha District Systems Restoration Team. In December, Congress passed the Disaster Relief Appropriations Act, which provided $1.7 billion to the corps for flood-related repairs. The Omaha District received $534 million of that total. Levee rehabilitation is expected to be completed by March. The Corps has awarded 98 contracts totaling $145 million for repairs to dams and navigation channel structures, with another four contracts expected to cost $56 million yet to be awarded. The majority of work at the dam projects is expected to be done by the end of 2014. Channel-control structure repairs are expected to be done in 2015. Source: http://siouxcityjournal.com/news/local/a1/corps-progressing-on-missouri-river-repairs/article_627265a9-49b5-52e3-8420-0dd068028d8d.html

Homeland Security Contacts

To report a homeland security incident, please contact your local law enforcement agency or one of these agencies: North Dakota State and Local Intelligence Center: 866-885-8295(IN ND ONLY); Email: ndslic@nd.gov; Fax: 701-328-8175 State Radio: 800-472-2121; Bureau of Criminal Investigation (BCI): 701-328-5500; North Dakota Highway Patrol: 701-328-2455; US Attorney's Office Intel Analyst: 701-297-7400; Bismarck FBI: 701-223-4875; Fargo FBI: 701-232-7241.

To contribute to this summary or if you have questions or comments, please contact:

Kirk Hagel, ND Division of Homeland Security kihagel@nd.gov, 701-328-8168